Image Steganography Based on Swarm Intelligence Algorithms: A Survey

Dilovan Asaad Zebari[1], Diyar Qader Zeebaree[2], Jwan Najeeb Saeed[3],Nechirvan Asaad Zebari[4], Adel AL-Zebari[5]

[1,2]Research Center of Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq
[3]IT Department, Duhok Technical Institute, Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq
[4]Electrical & Electronic Engineering Duhok Polytechnic University, Duhok, Kurdistan
Department of Computer Engineering, Harran University, Sanliurfa, Turkey
[5]Dept. of Information Technology, Technical College of Informatics, Duhok Polytechnic University, Kurdistan Region, Iraq.

Article Info
Volume 83
Page Number: 22257 – 22269
Publication Issue:
May-June 2020

Abstract

Information security and confidentiality are the prime concern of any type of communication. The techniques that utilizing inconspicuous digital media such as text, audio, video and image for hiding confidential data in it are collectively called Steganography. The key challenge of steganographic system design is to maintain a fair trade-off between, security, robustness, higher bit embedding rate and imperceptibility. Thus, with the massive progress in digital technology, to transmit secret messages through the internet effective steganography algorithms are required. However, the object which has been used to hide secret messages within may be exposed by compression or any type of noise which leads to extract secret message incorrectly. Therefore, utilizing the non-traditional basics for information security is required, such as swarm intelligence algorithms which are focused as a new aspect to achieve better security. In this paper, a survey of recent swarm intelligence algorithms based on steganography is covered. The objective function for swarm intelligence algorithms is realized in a way that the quality and robustness of the object that has been used for hiding messages are acceptable. With a particular emphasis on the main purpose and the objective of the proposed method based on the particular swarm intelligence algorithm has been reviewed. To present a more secure, efficient steganography algorithm based on swarm intelligence algorithms for future work, this will be helpful.

Article History
Article Received: *11 May 2020*
Revised: *19 May 2020*
Accepted: *29 May 2020*
Publication: *12 June 2020*

Keywords: *Data security, Image Steganography, Swarm Intelligence Algorithms.*

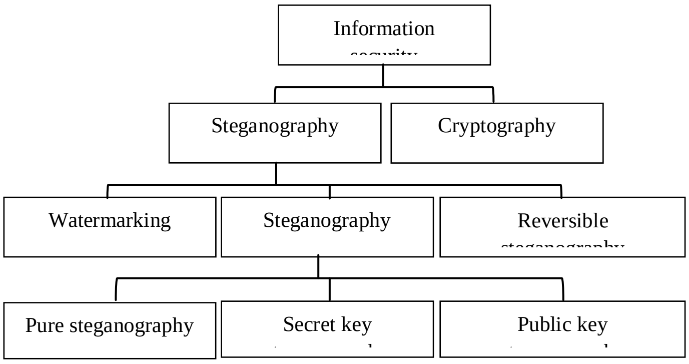
I. Introduction

Information security was among the most central issues that attracted much consideration as it played a significant role in every-day life. This concern has grown considerably following the advent of computers, particularly when the computer was adopted in nearly all spheres of modern life. Computer security is a broad label for the array of methods, measures, and devices proposed to shield, secure and safeguard computer systems alongside their information and data from hackers by discouraging them from attempting to access such systems without authorization [1, 2]. Essentially, information security classified into two main parts cryptography and information hiding. Information hiding is considered a key discipline of information security. Information hiding is a science used for secret communication among the source and the destination to protect secret data from a third party [3, 2].

Essentially, cryptography and steganography technologies are used to provide secret communication. However, steganography and cryptography differ considerably, Figure 1 showes the classification of the information security types. Both, of them technologies are utilized to achieve the different target. Cryptography is made up of two Greek words "kryptos" is meaning (hidden) and "graphein" is meaning (to write) [4, 2].The main goal of cryptography is to protect the secret message from unauthorized users by changing the real meaning of it into the unintelligible format without using any carrier which is called cipher message. In cryptography, the system will be break if the intruder can find the real meaning of the secret message which is called cryptanalysis. Therefore, the cryptosystem makes doubt in the mind of attackers because the cipher message is still known even after the encryption process. In contrast, steganography has been used to avoid the attacker's doubt [5, 6, 7, 8,9].

Fig 1: Classification of Information Security Types

The steganography notion is usually constructed by a pair of algorithms which are hiding and extracting secret message as shown in Figure 2.



Steganography is one of the main areas of information hiding technologies. t is composed of two Greek words "steganos" which is means covered or secret, and "graphy" which is means writing. The main goal of steganography is to conceal the private or sensitive information within different carries. In steganography, the secret message must be converted into a binary system to embed it. Therefore, the breaking steganography system (steganalysis), will be done if the intruder detects the hidden message. Aa a result, steganography is considered as a higher security level than cryptography in terms of the braking system because the presence of secret messages cannot be known by unauthorized people [7, 8, 9].

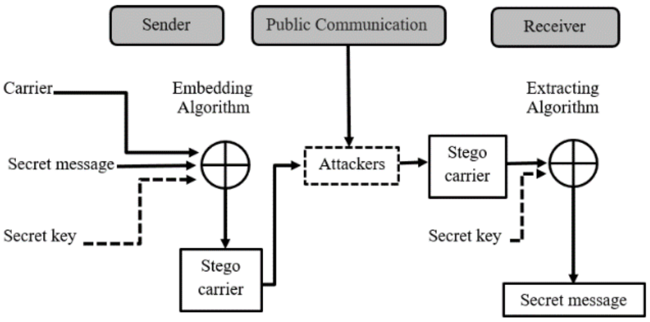


Fig 2: General Process of Steganography [12]

Throughout history, steganography has been utilized in ancient Greece and China in different forms [13]. During 440 B.C., an ancient common method of Greek had been demonstrated by Histaeus for hiding message. He used the head of trusted slaves to conceal the secret message. The secret information has been tattooed on the slave's scalp after shaving his hair. After growing slave's hair again, he was sent with the secret message to the destination place. The message cannot be detecting until the hair shaved again. Also, around 480 B.C., Demerstus used a wooden wax tablet to hide the message. In the process of his technique the secret message was written on the wood after taking off the wax and then covered the wood again with fresh wax [11, 12]. The stomach of rabbits is utilized for a hidden message, too [16]. Moreover, Jérôme Cardan invented another method to conceal the information. In his method, a masking paper that contains holes and blank paper was used as it is shown in Figure 2.2, mask located on the left side, cover located in the middle, and message located on the left side. In the process of hidden message, the mask was put on the blank paper and the message was written through the holes. After that, they were taking the mask and filled the blanks to appear the secret message [14, 15].

II. Steganography Types

In general, the steganography systems are divided into three main categories based on the steganography methods. The main goal of them is to embed secret information within any carrier in different ways. Using each type with any method a stego carrier will be obtained but in the different levels of security. As it is illustrated in Figure 1 there are three types of steganography are pure steganography, secret key steganography, and public key steganography.

A. Pure Steganography

Pure steganography is considered as one of the steganography systems. After combining specific carriers with a secret message by using any steganography technique the stego carrier will be obtained. Therefore, the process of this type does not require any secret key during the embedding process. Consequently, this type is considered as a mush less secure method because no key is involved. Thus, the security in this type is based on the privacy of the algorithm[16, 17].

B. Secret Key Steganography

Secret key steganography is considered an important type for protecting secret data from a third party. Unlike the previous type, the system of steganography in this type requiresa single secret key, this same key is also called a private or symmetric key. Therefore, the sender and receiver use the same key during carried out of both hiding and extraction. The main purpose of utilizing the key is to make the system more secure because of no one able to extract the secret message and read it only the one who has the key[21]. One of the great advantages of the private key is providing a fast process in both procedures. On the other hand, the drawback of this key is the system will become in risk if the key discovered by unauthorized users. Thus, this type of key should be changed considerably to keep the system securely [22]. The private key was the first type of key used in encryption before developing the public key in 1970 [23].

C. Public Key Steganography

Public key steganography is also known as an asymmetric key. Unlike the previous type of steganography, in this type pair of keys are used one for embedding and another for extraction to provide multiple levels of security during public communication. The key which is utilized by the transmitter to conceal the secret information within the carrier is called the public key. However, the other key utilized by the receiver during extracting the secret message is labeled as a private key. Both of keys are mathematically related to each other because they are generated together. The main advantage of this type of steganography is providing more robust for the system because even one key is known, it is hard to find the other key by a third party [17, 21]. On the other hand, the main problem of theasymmetric key is slower than the private key about 100-1000 times. Also, the public key systems exposed to more efficient attacks due to the publishing of the key [19, 22].

III. Steganography Applications

Several applications represent a container of sensitive information. These applications are used as cover objects or carriers in the steganography systems as it is shown in Figure 3. Every carrier has it is own characteristics to serve the steganography technology. Also, steganography technology needs a sufficient region in each carrier to protect the secret data. Also, the amount of secret information to conceal within each carrier depends on the availability of the region of the specific carrier. Therefore, carriers are represented as an essential ingredient in steganography technology because they are determining the amount of data that can be hidden. Furthermore, to conceal the secret data within each carrier some parts of them will be manipulated by using different algorithms. However, maintain the accuracy and stay the format intact of each carrier after the embedding process or maybe modifying some parts of them to stay imperceptible to unauthorized people in public communication.

A. Text steganography

Historically, the text was an obvious carrier used to protect secret data from unauthorized people. Utilizing text as a carrier was the most important steganography method. In this method, each bit of secret data was concealed in every nth letter of text carrier. After increasing the using of the internet and discovering some other carriers, the significance of using text as a carrier among researchers is decreased because of a very small amount of redundant data compared with other carriers. However, stego text which obtaining after embedding secret data is often more imperceptible than other digital carriers [20, 26]. The main benefit of using text as a carrier in steganography system is that, it does not require much memory also it is easy to transfer [23, 24]. Several algorithms have been used to embed the secret message within the text such as open space methods [5], syntactic methods, semantic methods [29], shift coding [30], and feature coding [27, 28].

B. Video steganography

Videos also as images are very common choice were used to hide secret information as a carrier. Steganography video is very effective and successful due it is a high capacity more than image capacity. Many different video file formats can be used in the domain of steganography videos such as Moving Picture Experts Group (MPEG), MP4, and Audio Video Interleave (AVI) [29, 30, 32]. Generally, steganography in the video is classified into two main types which are uncompressed and compressed video. Essentially, hiding information in the video is similar to hiding information in an image where the data will be hidden within different frames of video (Chandel, 2016). Consequently, techniques of steganography in an image can also be applied on video [29, 31, 32, 33]. Especially, Discrete Cosine Transform (DCT) is the most common technique has been used in video steganography to achieve high security and high visual quality [39].

C. Audio steganography

In the field of information hiding, audio files have been utilized as a carrier for embedding secret data in digital sound. The process of steganography in audio will be done by changing the binary sequence of a sound file slightly. Hiding data in audio is usually harder than concealing data in other carriers. Different audio files have been used for protecting secret information such as WAV, AU, and even MP3 [16][10,26]. Several algorithms have been presented to embed secret information within audio files successfully. List Significant Bit (LSB) coding, Parity coding, Phase coding, Spread Spectrum, and Echo coding are the most common methods were used to hide data in audio files [35, 36, 37, 38, 39].

D. Image steganography

Over the past few years, digital images became popular carriers for hiding secret information to prevent from unauthorized users. Since the 1990s, we have seen a remarkable development in digital image processing. Due to high capacity in images, a low impact on the visibility, and the simplicity of their manipulation have attracted many researchers to work in the field of information hiding for digital images. Many different image formats can be used in the domain of image steganography such as Graphics Interchange Format (GIF), Windows Bitmap (BMP), Joint Photographic Expert Group (JPEG), and so on [29, 40]. Based on the spatial domain and transform domain several steganography techniques have been used for embedding secret data within the digital images efficiently. Recently, in the spatial domain immense schemes based on LSB technique [41, 24], Optimal Pixel Adjustment (OPA) technique [46,47], and Pixel Value Differencing (PVD) [49] have been proposed. Moreover, in the transform domain several methods based on the Discrete Cosine Transform (DCT) technique [50, 51] and Discrete Wavelet Transform (DWT) technique [52] have been presented. Furthermore, to increase the security level some researchers proposed a hybrid scheme by combining both spatial and transform domains [46, 47, 52].

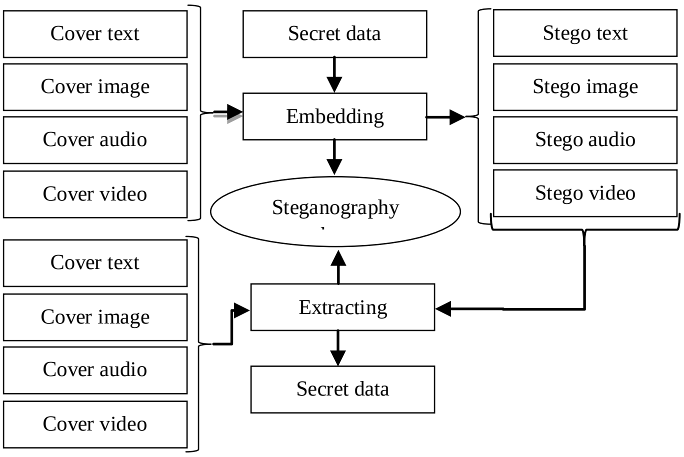


Fig 3: Bock Diagram of Steganography Application

Iv. Swarm Intelligence Algorithms in Steganography

Swarm intelligence (SI) is a relatively novel line of research Artificial Intelligence (AI)[48, 50,54]. Natural biological simulations motivated (SI) through a set of locally naïve interrelated vehicles that react with the surrounding setting [59]. In the last period, a few SI algorithms, like PSO, FA, and ABC made various significant applications to the domain of steganography[51, 52], the mechanism of hiding secret message based on swarm intelligence algorithms has been illustrated in Figure 4. To preserve the quality of the image many techniques have been used with steganography in image. After that, metaheuristic algorithms named swarm intelligence algorithms have been used with images to find the best location where the secret message can be embedded as well as payload capacity.

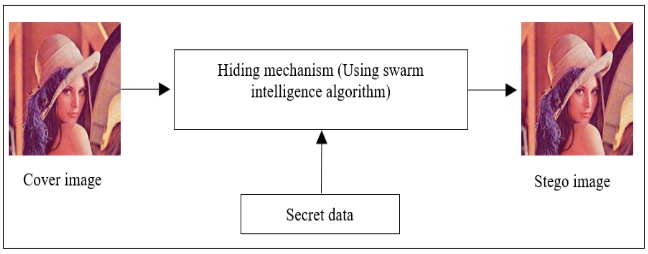


Fig4: Steganography Mechanism Using Swarm Algorithms

A. Ant Colony Optimization (ACO)

Ant Colony Optimization (ACO) [62] algorithm patterns the conduct of ants scrounging. It is valuable for issues that need figuring out the most express route as an objective. Practically, when ants discover their surrounding area, it leaves the pheromones to guide each other toward nutrients. ACO likewise recreates this strategy and every ant saves correspondingly its location to make more ants pinpoint better arrangements in future cycles. This pattern proceeds until the optimal route is established. Ants to construct their trip, their behavior is going via the vertices in the graph. Assume that the nest will be left by ants to find food. There are four various paths to four various vertices v00, v10, v20 and v30, as shown in Figure 5.

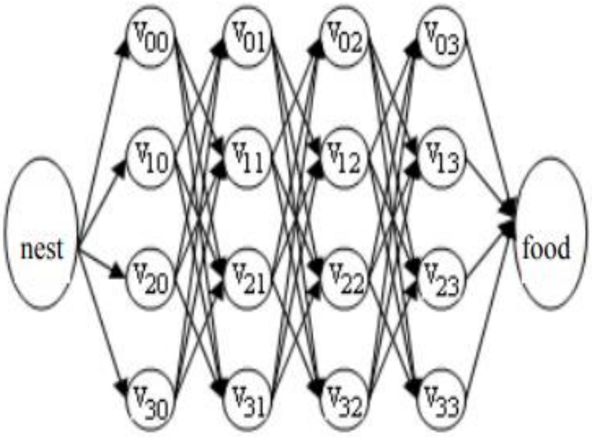


Fig 5: The Behavious of Ant Colony

B. Firefly Algorithm (FA)

Figure 6 illustrates Firefly Algorithm (FA) was promoted by Xin-She Yang in 2008, which depended on the glimmering examples and conduct of tropical fireflies. FA is straightforward, adaptable, and undemanding to actualize [63]. It may be utilized for limited optimization works. The glimmering conduct of fireflies occurs as a result of the bioluminescence process. Fireflies are capable of controlling their glimmering conduct relying on an exterior incentive. This process is utilized to draw in other members of their species or prey. In a Firefly algorithm, a population of fireflies is counted. The power of light that they emanate determines the attraction between fireflies. The flying insects with the greatest glow may attract more fireflies. The solution space is drawn on to these insects and the nature of the arrangement of every firefly is straightforwardly relative to its lighting level. Hence, fireflies that have better arrangements pull in its cohorts (paying little attention to their sex), this means that exploring the hunt space will be more well-organized[64].

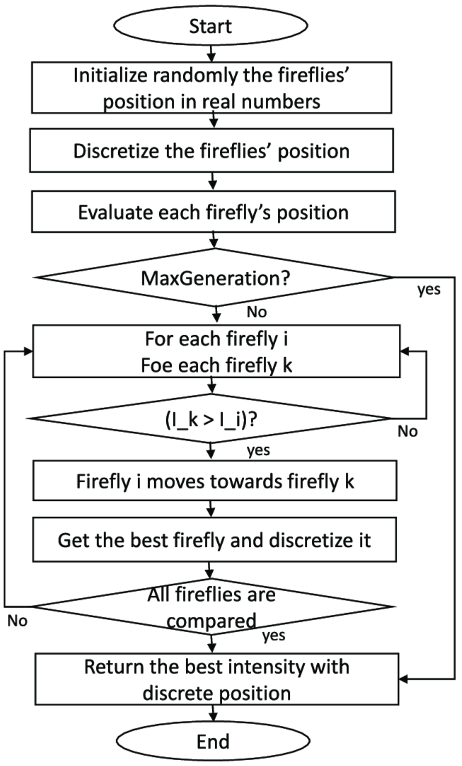

Start
Initialize randomly the fireflies' position in real numbers
Discretize the fireflies' position
Evaluate each firefly's position
MaxGeneration?
yes
No
For each firefly i
Foe each firefly k
(I_k > I_i)?
No
yes
Firefly i moves towards firefly k
Get the best firefly and discretize it
All fireflies are compared
No
yes
Return the best intensity with discrete position
End

Fig 6: The General Concept of Firefly Algorithm

C. Artificial Bee Colony (ABC)

The Artificial Bee Colony (ABC) algorithm is one more population-dependent offered by [65]. This algorithm emulates the smart conduct of honeybees and harnesses triple stages to locate the best arrangement: working honeybee, passerby honeybee, and scout honeybee stages. Working and passerby honeybees possess local seeking everywhere in the area and pick nutrient-based on the deterministic and probabilistic determination in their stages correspondingly. They pick nutrients in light of their knowledge and their home mates and adjust their locations. In the Scout stage, scout honeybees fly and pick the nutrients arbitrarily without resorting to prior experience. If the quantity of nectar in a new source is greater than that of the past one that is saved in their memory, they keep the new location and disremember the earlier one. In this way, ABC offsets exploration and exploitation process with local and universal exploration techniques on working, passerby, and scout's stages and gets the best arrangement. Figure 7 ABC algorithm has an asset in local and universal quests. Additionally, it is actualized in a few optimization issues.

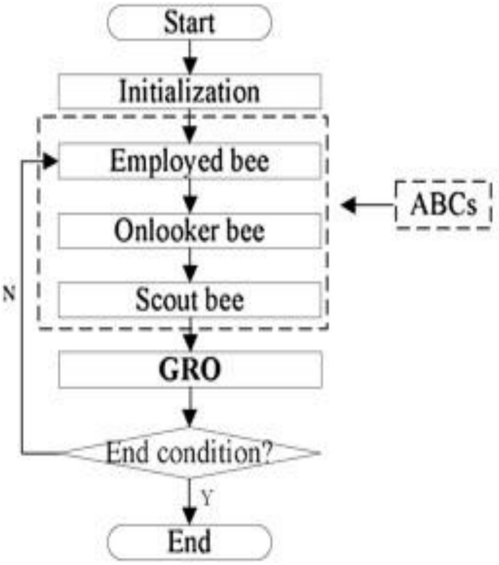


Fig 7: The Behaviors of Artificial Bee Colony

D. Particle Swarm Optimization (PSO)

Particle Swarm Optimization (PSO) is a fruitful swarm intelligence strategy that relies on the capacity of assemblies. It turned out to be extremely famous nowadays as an effective search and optimization method. This procedure can be implemented where a question is raised, and its answer can be acquired from multiple means. PSO does not need any gradient knowledge about the function that will undergo optimization, and it utilizes just primitive numerical operators and its conception is extremely straightforward [57, 58, 59] PSO was presented by Russell Eberhart, an electrician, and James Kennedy, a social analyst, in 1995 [60, 61]. It is motivated by the smart, encounter sharing, social-assembling conduct of birds, and it was initially replicated on a PC by Craig Reynolds, and further examined by Frank Heppner [62, 63]. Figure 8 shows PSO has drawn the consideration of a great deal of scholars throughout the world coming which resulted the introduction of countless fundamental versions of the algorithm and also numerous parameter computerization techniques [59,77, 65].

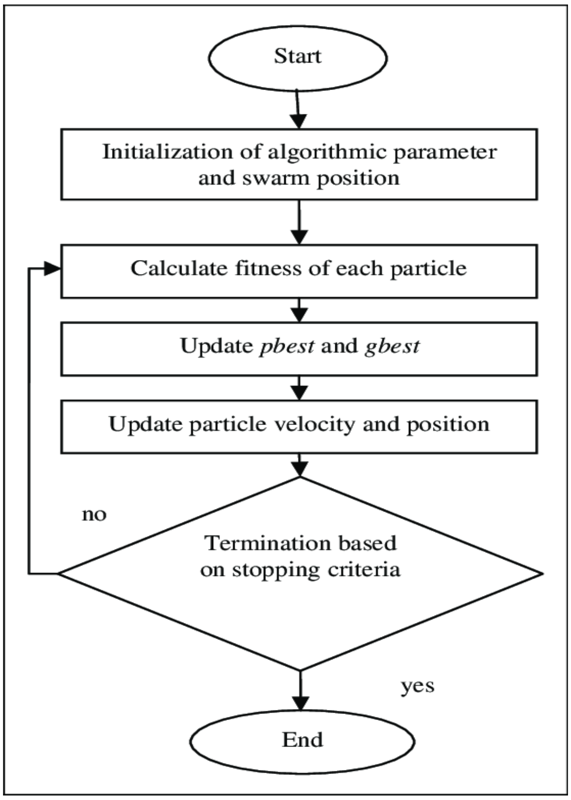

Start
Initialization of algorithmic parameter and swarm position
Calculate fitness of each particle
Update *pbest* and *gbest*
Update particle velocity and position
no
Termination based on stopping criteria
yes
End

Fig 8: The process of PSO Algorithm

Table I briefly reviews the swarm intelligence algorithms used with steganography in the image. In this table, the purpose of using existing algorithm as well as the objective of applying swarm algorithm in this domain.To preserve the quality of the image many techniques have been used with steganography in image. After that, metaheuristic algorithms named swarm intelligence algorithms have been used with images to find the best location where a secret message can be embedded as well as payload capacity. Table I briefly reviews the swarm intelligence algorithms used with steganography in the image. In this table, the purpose of using existing algorithm as well as the objective of applying swarm algorithm in this domain.

Table I: Swarm Intelligence Algorithms with Steganography in Image

feR	mhtiroglA	rof desU	evitcejbO
[74]	PSO	For converting secret data, the best substitution matrix has been found	To ameliorate the quality of stego carrier
[75]	PSO	For any 8*8 block of the carrier the best substitution matrix has been found rather than only one matrix for the entire carrier then the convert the secret data by these matrices	In order to increase the security, preserve quality, and more embedding capacity
[76]	ACO	Helped to build the best LSB substitution matrix to obtain the new secret message	In order to preserve the quality and to obtain more effectiveness
[77]	PSO	Used in three schemes to obtain the best conversion matrix T	First scheme to increase the security while other schemes to ameliorate the quality of stego
[20]	PSO	Producing the secret key also to select the best pixel in cover image	Ameliorated the performance of LSB and to reach the better quality.
[77]	PSO	The best pixel positions selected to embed the pixels of secret image	To preserve the quality of stego image as well as the robustness
[78]	PSO	To choose the global best location for concealing data	In order to increase the hiding capacity where more data can be hidden
[79]	PSO andACO	To obtain the optimized edged cover and the optimum pixels of image are selected for embedding	In order to preserve the quality and better security of stego image
[80]	PSO	To select the best LSBs of carrier to embed the Most Significant Bit (MSB) of secret data as well as to find a key	In order to enhance the performance of concealing
[81]	Firefly	To select the optimum position	In order to preserve the quality of image
[82]	PSO	Used to conceal data within an image based on DWT	In order to obtain the highest PSNR and better payload capacity
[83]	PSO	Analyzing the hiding process to select the position of pixels for embedding the data	In order to enhance the capacity and the performance
[84]	ACO	The best set of pixel bits in carrier has been found to substitute with the secret data bits	In order to present an efficient steganography method and comparison among Genetic Algorithm (GA) and ACO
[85]	ABC	The best solution has been calculated in order to conceal the secret data within it	To increase hiding capacity and to preserve the quality
[68]	PSO	Used to embed the message within Integer Wavelet Transform (IWT) coefficients of the carrier and to generate a key	To obtain more security, robustness, and the quality of stego carrier

V. CONCLUSION

In steganography technologies, the bits of the secret message should be encoded effectively, and the quality of the image should be preserved efficiently. Many researchers worked to hide secret messages in an image based on different technologies. Several approaches have been proposed and used to hide secret messages in an image. Thus, a review of several image steganography based on swarm intelligence algorithms has been presented in this paper. The main purpose of this paper is to show the importance of using swarm intelligence algorithms in image steganography. The swarm intelligence algorithm which has been used in the proposed work has been indicated. More so, the issue of the swarm intelligence algorithm used in previous studies has been introduced. Finally, the main objective of the previous studies has been cleared.

VI. References

[1] A. Al - Wattar, “DYNAMIC key-depending S-boxes inspired by biological DNA,” *Int. J. Electr. Comput. Sci. IJECS*, vol. 15, no. 04, pp. 48–53, 2015.

[2] Zeebaree, D. Q., Haron, H., Abdulazeez, A. M., & Zebari, D. A. (2019, April). Machine learning and Region Growing for Breast Cancer Segmentation. In 2019 International Conference on Advanced Science and Engineering (ICOASE) (pp. 88-93). IEEE.

[3] H. Singh and D. Singh, “Location based information hiding,” presented at the 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA)(Spring), 2016, pp. 1–4.

[4] Zebari, D. A., Haron, H., Zeebaree, S. R., & Zeebaree, D. Q. (2018, October). Multi-Level of DNA Encryption Technique Based on DNA Arithmetic and Biological Operations. In 2018 International Conference on Advanced Science and Engineering (ICOASE) (pp. 312-317). IEEE.

[5] Shivani, V. Yadav, and S. Batham, “A Novel Approach of Bulk Data Hiding using Text Steganography,” in *Procedia Computer Science*, 2015, vol. 57, pp. 1401–1410.

[6] A. Al-Zebari and A. Sengur, “Performance Comparison of Machine Learning Techniques on Diabetes Disease Detection,” presented at the 2019 1st International Informatics and Software Engineering Conference (UBMYK), 2019, pp. 1–4.

[7] Zeebaree, D. Q., Haron, H., & Abdulazeez, A. M. (2018, October). Gene selection and classification of microarray data using convolutional neural network. In 2018 International Conference on Advanced Science and Engineering (ICOASE) (pp. 145-150). IEEE.

[8] O. Ahmed and A. Brifcani, “Gene Expression Classification Based on Deep Learning,” presented at the 2019 4th Scientific International Conference Najaf (SICN), 2019, pp. 145–149.

[9] N. Najat and A. M. Abdulazeez, “Gene clustering with partition around mediods algorithm based on weighted and normalized Mahalanobis distance,” presented at the 2017 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), 2017, pp. 140–145.

[10] Sulaiman, D. M., Abdulazeez, A. M., Haron, H., & Sadiq, S. S. (2019, April). Unsupervised Learning Approach-Based New Optimization K-Means Clustering for Finger Vein Image Localization. In 2019 International Conference on Advanced Science and Engineering (ICOASE) (pp. 82-87). IEEE.

[11] A. Al-Mohammad, “Steganography-based secret and reliable communications: Improving steganographic capacity and imperceptibility,” 2010.

[12]D. A. Zebari, H. Haron, D. Q. Zeebaree, and A. M. Zain, ‘A Simultaneous Approach for Compression and Encryption Techniques Using Deoxyribonucleic Acid’, presented at the 2019 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), 2019, pp. 1–6.

[13]Y. Wang and P. Moulin, “Optimized feature extraction for learning-based image steganalysis,” *IEEE Trans. Inf. Forensics Secur.*, vol. 2, no. 1, pp. 31–45, 2007.

[14] Zebari, D. A., Haron, H., Zeebaree, S. R., & Zeebaree, D. Q. (2019, April). Enhance the Mammogram Images for Both Segmentation and Feature Extraction Using Wavelet Transform. In *2019 International Conference on Advanced Science and Engineering (ICOASE)* (pp. 100-105). IEEE.

[15] V. Kumar, “A Study on Steganography & Data Hiding,” *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 3, no. 10, pp. 9504–9513, 2015.

[16] S. K. Bandyopadhyay, D. Bhattacharyya, D. Ganguly, S. Mukherjee, and P. Das, “A tutorial review on steganography,” presented at the International conference on

contemporary computing, 2008, vol. 101, pp. 105–114.

[17] A. Cheddad, “Steganoflage: a new image steganography algorithm,” 2009.

[18] N. Adeen, M. Abdulazeez, and D. Zeebaree, “Systematic Review of Unsupervised Genomic Clustering Algorithms Techniques for High Dimensional Datasets,” vol. 62, no. 3, 2020.

[19] J. Ashok, Y. Raju, S. Munishankaraiah, and K. Srinivas, “Steganography: an overview,” *Int. J. Eng. Sci. Technol.*, vol. 2, no. 10, pp. 5985–5992, 2010.

[20] A. M. Nickfarjam and Z. Azimifar, “Image steganography based on pixel ranking and particle swarm optimization,” presented at the The 16th CSI International Symposium on Artificial Intelligence and Signal Processing (AISP 2012), 2012, pp. 360–363.

[21] Sheelu and B. Ahuja, “An Overview of Steganography,” *IOSR J. Comput. Eng. IOSR-JCE*, pp. 15–19, 2013.

[22] A. Khalifa, “LSBase: A key encapsulation scheme to improve hybrid crypto-systems using DNA steganography,” presented at the 2013 8th International Conference on Computer Engineering & Systems (ICCES), 2013, pp. 105–110.

[23] S. William, *Cryptography and Network Security: for VTU*. Pearson Education India, 2006.

[24] S. Jain and V. Bhatnagar, “Analogy of various DNA based security algorithms using cryptography and steganography,” presented at the 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014, pp. 285–291.

[25] M. R. N. Torkaman, N. S. Kazazi, and A. Rouddini, “Innovative approach to improve hybrid cryptography by using DNA steganography,” *Int. J. New Comput. Archit. Their Appl.*, vol. 202, pp. 225–236, 2012.

[26] S. I. Saleem, S. R. Zeebaree, D. Q. Zeebaree, and A. M. Abdulazeez, “Building Smart Cities Applications based on IoT Technologies: A Review,Vol 62,03,2020.”

[27] S. Bansod and G. Bhure, “Data encryption by image steganography,” *Int J Inf. Comput Technol Int Res Publ House*, vol. 4, pp. 453–458, 2014.

[28] D. M. Abdulqader, A. M. Abdulazeez, and D. Q. Zeebaree, “Machine Learning Supervised Algorithms of Gene Selection: A Review,” *Mach. Learn.*, vol. 62, no. 03, 2020.

[29] M. H. Shirali-Shahreza and M. Shirali-Shahreza, “A new approach to Persian/Arabic text steganography,” presented at the 5th IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse (ICIS-COMSAR’06), 2006, pp. 310–315.

[30] Y.-W. Kim, K.-A. Moon, and I.-S. Oh, “A Text Watermarking Algorithm based on Word Classification and Inter-word Space Statistics.,” presented at the ICDAR, 2003, pp. 775–779.

[31] K. F. Rafat, “Enhanced text steganography by changing word’s spelling,” presented at the Proceedings of the 7th International Conference on Frontiers of Information Technology, 2009, pp. 1–4.

[32] D. Q. Zeebaree, H. Haron, A. M. Abdulazeez, and D. A. Zebari, “Trainable Model Based on New Uniform LBP Feature to Identify the Risk of the Breast Cancer,” presented at the 2019 International Conference on Advanced Science and Engineering (ICOASE), 2019, pp. 106–111.

[33] K. U. Singh, “Video steganography: text hiding in video by LSB substitution,” *Int. J. Eng. Res. Appl.*, vol. 4, no. 5, pp. 105–108, 2014.

[34] A. M. A. Brifcani and J. N. Al-Bamerny, “Image compression analysis using multistage vector quantization based on discrete wavelet transform,” presented at the 2010 International Conference on Methods and Models in Computer Science (ICM2CS-2010), 2010, pp. 46–53.

[35] J. N. Saeed, “A SURVEY OF ULTRASONOGRAPHY BREAST CANCER

IMAGE SEGMENTATION TECHNIQUES," *Acad. J. Nawroz Univ.*, vol. 9, no. 1, pp. 1–14, 2020.

[36] V. M. Wajgade and D. S. Kumar, "Enhancing data security using video steganography," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 3, no. 4, pp. 549–552, 2013.

[37] S. Khupse and N. N. Patil, "An adaptive steganography technique for videos using Steganoflage," presented at the 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014, pp. 811–815.

[38] R. Kaur and S. Kaur, "XOR-EDGE based video steganography and testing against chi-square steganalysis," *Int. J. Image Graph. Signal Process.*, vol. 8, no. 9, p. 31, 2016.

[39] M. S. Kumar and G. M. Latha, "DCT based secret image hiding in video sequence," *J. Eng. Res. Appl. Www Ijera Com ISSN*, pp. 2248–9622, 2014.

[40] R. M. Nugraha, "Implementation of direct sequence spread spectrum steganography on audio data," presented at the Proceedings of the 2011 International Conference on Electrical Engineering and Informatics, 2011, pp. 1–6.

[41] A. K. Mandal, M. Kaosar, M. O. Islam, and M. D. Hossain, "An approach for enhancing message security in audio steganography," presented at the 16th Int'l Conf. Computer and Information Technology, 2014, pp. 383–388.

[42] S. Bhalshankar and A. K. Gulve, "Audio steganography: LSB technique using a pyramid structure and range of bytes," *ArXiv Prepr. ArXiv150902630*, 2015.

[43] R. Chowdhury, D. Bhattacharyya, S. K. Bandyopadhyay, and T. Kim, "A view on LSB based audio steganography," *Int. J. Secur. Its Appl.*, vol. 10, no. 2, pp. 51–62, 2016.

[44] S. R. Zeebaree, R. R. Zebari, K. Jacksi, and D. A. Hasan, "Security Approaches For Integrated Enterprise Systems Performance: A Review."

[45] Y. Yang, "Information analysis for steganography and steganalysis in 3D polygonal meshes," 2013.

[46] G. Manjula and A. Danti, "A novel hash based least significant bit (2-3-3) image steganography in spatial domain," *ArXiv Prepr. ArXiv150303674*, 2015.

[47] P. K. Gupta, R. Roy, and S. Changder, "A secure image steganography technique with moderately higher significant bit embedding," presented at the 2014 International Conference on Computer Communication and Informatics, 2014, pp. 1–6.

[48] N. N. Mohammed and A. M. Abdulazeez, "Evaluation of partitioning around medoids algorithm with various distances on microarray data," presented at the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017, pp. 1011–1016.

[49] H. Al-Dmour, A. Al-Ani, and H. Nguyen, "An efficient steganography method for hiding patient confidential information," presented at the 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2014, pp. 222–225.

[50] A. Mondal and S. Pujari, "A novel approach of imagebased steganography using pseudorandom sequence generator function and DCT coefficients," *Int. J. Comput. Netw. Inf. Secur.*, vol. 7, no. 3, pp. 42–49, 2015.

[51] S. S. Sadiq, A. M. Abdulazeez, and H. Haron, "Solving multi-objective master production schedule problem using memetic algorithm," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 18, no. 2, pp. 938–945, 2020.

[52] R. S. Naoum, "Image Steganography Based on Discrete Wavelet Transform and Enhancing Resilient Backpropogation Neural Network," 2015.

[53] K. S. Shete, M. Patil, and J. Chitode, "Least significant bit and discrete wavelet transform algorithm realization for image steganography

employing FPGA," *Int. J. Image Graph. Signal Process.*, vol. 8, no. 6, p. 48, 2016.

[54] M. Mahdi Hashim, M. Rahim, and M. Shafry, "IMAGE STEGANOGRAPHY BASED ON ODD/EVEN PIXELS DISTRIBUTION SCHEME AND TWO PARAMETERS RANDOM FUNCTION.," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 22, 2017.

[55] M. R. Mahmood, A. M. Abdulazeez, and Z. Orman, "Dynamic Hand Gesture Recognition System for Kurdish Sign Language Using Two Lines of Features," presented at the 2018 International Conference on Advanced Science and Engineering (ICOASE), 2018, pp. 42–47.

[56] J. Ghorpade-Aher and V. A. Metre, "Clustering Multidimensional Data with PSO based Algorithm," *ArXiv Prepr. ArXiv14026428*, 2014.

[57] I. M. Zeebaree, D. Q. Zeebaree, and Z. A. Ayoub, "FACE RECOGNITION USING STATISTICAL FEATURE EXTRACTION AND NEURAL. Vol 62,03,2020."

[58] A. S. Eesa, Z. Orman, and A. M. A. Brifcani, "A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems," *Expert Syst. Appl.*, vol. 42, no. 5, pp. 2670–2679, 2015.

[59] S. Roy, S. Biswas, and S. S. Chaudhuri, "Nature-inspired swarm intelligence and its applications," *Int. J. Mod. Educ. Comput. Sci.*, vol. 6, no. 12, p. 55, 2014.

[60] S. M. Thampi, "Information hiding techniques: a tutorial review," *ArXiv Prepr. ArXiv08023746*, 2008.

[61] R. Zebari, A. Abdulazeez, D. Zeebaree, D. Zebari, and J. Saeed, "A Comprehensive Review of Dimensionality Reduction Techniques for Feature Selection and Feature Extraction," *J. Appl. Sci. Technol. Trends*, vol. 1, no. 2, pp. 56–70, 2020.

[62] M. Dorigo, V. Maniezzo, and A. Colorni, "Ant system: optimization by a colony of cooperating agents," *IEEE Trans. Syst. Man Cybern. Part B Cybern.*, vol. 26, no. 1, pp. 29–41, 1996.

[63] X.-S. Yang, "Swarm intelligence based algorithms: a critical analysis," *Evol. Intell.*, vol. 7, no. 1, pp. 17–28, 2014.

[64] N. Kayarvizhy, S. Kanmani, and R. Uthariaraj, "ANN models optimized using swarm intelligence algorithms," *WSEAS Trans. Comput.*, vol. 13, no. 45, pp. 501–519, 2014.

[65] D. Karaboga, "An idea based on honey bee swarm for numerical optimization," Technical report-tr06, Erciyes university, engineering faculty, computer …, 2005.

[66] T. Yu, L. Wang, X. Han, Y. Liu, and L. Zhang, "Swarm intelligence optimization algorithms and their application," *WHICEB 2015 Proc*, vol. 3, 2015.

[67] S. Das, A. Abraham, and A. Konar, "Swarm intelligence algorithms in bioinformatics," in *Computational Intelligence in Bioinformatics*, Springer, 2008, pp. 113–147.

[68] S. Thenmozhi and M. Chandrasekaran, "Novel Technology for Secure Data Transmission Based on Integer Wavelet Transform and Particle Swarm Optimization," *Res. J. Appl. Sci. Eng. Technol.*, vol. 12, no. 2, pp. 188–196, 2016.

[69] R. Eberhart and J. Kennedy, "A new optimizer using particle swarm theory," presented at the MHS'95. Proceedings of the Sixth International Symposium on Micro Machine and Human Science, 1995, pp. 39–43.

[70] K. J, "abd Eberhart R," in *proceedings of the IEEE*, 1995.

[71] H. Ahmed and J. Glasgow, "Swarm intelligence: concepts, models and applications," *Sch. Comput. Queens Univ. Tech. Rep.*, 2012.

[72] M. B. Abdulrazzaq and J. N. Saeed, "A Comparison of Three Classification Algorithms for Handwritten Digit Recognition," presented at the 2019 International Conference on Advanced Science and Engineering (ICOASE), 2019, pp. 58–63.

[73] O. M. S. Hassan, A. M. Abdulazeez, and V. M. TİRYAKİ, "Gait-based human gender classification using lifting 5/3 wavelet and

principal component analysis," presented at the 2018 International Conference on Advanced Science and Engineering (ICOASE), 2018, pp. 173–178.

[74] X. Li and J. Wang, "A steganographic method based upon JPEG and particle swarm optimization algorithm," *Inf. Sci.*, vol. 177, no. 15, pp. 3099–3109, 2007.

[75] S. Fazli and M. Kiamini, "A high_performance steganographic method using JPEG and PSO algorithm," presented at the 2008 IEEE International Multitopic Conference, 2008, pp. 100–105.

[76] C.-S. Hsu and S.-F. Tu, "Finding optimal LSB substitution using ant colony optimization algorithm," presented at the 2010 Second International Conference on Communication Software and Networks, 2010, pp. 293–297.

[77] P. Bedi, R. Bansal, and P. Sehgal, "Using PSO in a spatial domain based image hiding scheme with distortion tolerance," *Comput. Electr. Eng.*, vol. 39, no. 2, pp. 640–654, 2013.

[78] K. Jaidka and A. Mavi, "PSO (Particle Swarm Optimization) Based Reversible Data Hiding," *Int. J. Sci. Res. IJSR*, vol. 4, no. 6, pp. 2480–2483, 2015.

[79] N. Kaur and A. Garg, "Steganography Using PSO Based Hybrid Algorithm," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 1, 2014.

[80] A. Nickfarjam, H. Ebrahimpour-Komleh, and A. P. Najafabadi, "Image hiding using neighborhood similarity," presented at the 2014 6th Conference on Information and Knowledge Technology (IKT), 2014, pp. 79–82.

[81] A. Amsaveni and C. Arunkumar, "An efficient data hiding scheme using firefly algorithm in spatial domain," presented at the 2015 2nd International Conference on Electronics and Communication Systems (ICECS), 2015, pp. 650–655.

[82] E. Divya and P. Rajkumar, "Steganographic Data Hiding using DWT and Particle Swarm Optimization," *Int. J. Comput. Appl.*, vol. 117, no. 14, 2015.

[83] D. E and R. P, "Image To Image Hiding Using PSO," *Int. J. Innov. Res. Adv. Eng.*, vol. 2, no. 5, pp. 146–151, 2015.

[84] W. S. Awad, "Information hiding using ant colony optimization algorithm," *Int. J. Technol. Diffus. IJTD*, vol. 2, no. 1, pp. 16–28, 2011.

[85] A. Kaur, R. Kaur, and N. Kumar, "Image steganography using discrete wavelet transformation and artificial bee colony optimization," presented at the 2015 1st International Conference on Next Generation Computing Technologies (NGCT), 2015, pp. 990–994.